Department of Homeland Security Daily Open Source Infrastructure Report for 22 August 2005

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports a former Army National Guard reservist was sentenced to eight years in prison for stealing nearly 1,000 pieces of luggage at Washington, DC's three major airports. (See item 7)
- The Associated Press reports a virus caused the U.S. Customs computer system used to process passengers arriving on international flights to shut down for several hours on August 18, leaving long lines of impatient travelers. (See item 9)
- Agence France−Presse reports the World Health Organization warns that the global capacity to manufacture anti−flu vaccines would not be flexible or large enough to counter a threatened pandemic that could rapidly kill millions of people around the world. (See item 20)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *August 19, Pittsburgh Post−Gazette (PA)* — **Questions remain two years after massive blackout.** Two years ago, on August 14, the largest power outage in American history occurred. A Carnegie Mellon University (CMU) economist thinks that it not only could happen again, but that it most likely will. "Almost nothing has been done that would make it better,"

said Lester Lave, a professor of economics at CMU's Tepper School of Business. The reason, Lave said, is that neither the improvements made to the operation of America's power grid since the blackout nor additional changes included in the new energy bill address a fundamental problem in the way that electricity is delivered to American consumers. The problem, he said, is that the three stages of delivery are performed by separate parties that, though they may cooperate, are essentially independent. "Deregulation has tended to make things worse because you no longer had a utility that was responsible for providing reliability in its service area," Lave said. Instead, the reliability of the grid depends on the cooperation of and communication among the various providers. Lave suggests that grid operators need a facility such as the Federal Aviation Administration's Command Center that would continuously monitor data from across the country to help prevent future power problems.
Source: http://www.post−gazette.com/pg/05231/556260.stm

2. *August 19, The Tampa Tribune (FL)* — **Utilities avoid melting point.** The summer's stifling heat and humidity have sent demand for electricity soaring in the Tampa Bay, FL, area. However, utility officials have stayed confident that they can access enough power to keep air conditioners humming. Still, Tampa Electric Co. and Progress Energy have worked hard supplying enough electricity these past few weeks. There haven't been any brownouts or blackouts, however, the two utilities are edging close enough to maximum capacities that plans to boost power generating capacity over the next few years will be timely for a region that continues to grow dramatically. “There are a lot of areas for growth in our area, and we don't see it slowing down. It is a big challenge,” said Ben Crisp, Progress Energy Inc. director of system planning. The higher power demand is being driven by thousands of new customers moving into the territories of Tampa Electric and Progress Energy Florida annually. Each utility sees about a 2.5 percent increase in customers each year. Both companies are planning new power plants to help meet demand.
Source: http://www.tampatrib.com/MGB49NIRJCE.html

3. *August 19, Government Accountability Office* — **GAO−05−665: Securing U.S. Nuclear Materials: DOE Needs to Take Action to Safely Consolidate Plutonium (Report).** Plutonium is very hazardous to human health and the environment and requires extensive security because of its potential use in a nuclear weapon. The Department of Energy (DOE) stores about 50 metric tons of plutonium that is no longer needed by the United States for nuclear weapons. Some of this plutonium is contaminated metal, oxides, solutions, and residues remaining from the nuclear weapons production process. To improve security and reduce plutonium storage costs, DOE plans to establish enough storage capacity at its Savannah River Site (SRS) in the event it decides to consolidate its plutonium at SRS until it can be permanently disposed of in a geologic repository at Yucca Mountain, Nevada. The Government Accountability Office (GAO) was asked to examine (1) the extent to which DOE can consolidate this plutonium at SRS and (2) SRS’s capacity to monitor plutonium storage containers. GAO recommends that DOE (1) develop a comprehensive strategy to consolidate, store, and eventually dispose of its plutonium and (2) ensure that its facilities’ cleanup plans are consistent with its plutonium consolidation plans. In commenting on the report, DOE generally agreed with our recommendations.
Highlights: http://www.gao.gov/highlights/d05665high.pdf
Source: http://www.gao.gov/new.items/d05665.pdf

4. *August 18, Associated Press* — **Department of Energy plans to detonate truck bombs to test nuclear site security.** To test whether U.S. nuclear installations could withstand terrorist truck−bomb attacks, the federal government is planning to detonate two such bombs in the eastern Idaho desert. "The exact amount of explosives and the magnitude is classified, but we can say it will be no more than the equivalent of 15,000 pounds of TNT," Department of Energy (DOE) spokesperson Tim Jackson said on Wednesday, August 17, at the Idaho National Laboratory. In a draft environmental assessment the agency released Wednesday, DOE officials said the frequency, size and severity of car−bombing attacks against American targets compelled the agency to test whether nuclear site security barriers are vulnerable to explosives delivered by vehicles. Data collected from the Idaho tests will also be used by other federal agencies, as well as state and local governments, to understand the effects of vehicle bombs on security perimeters of potential terrorist targets. Officials want to detonate two bombs at the 890−square−mile Idaho nuclear research compound, the first this fall and the second early in 2006. The first test will focus on the effects of the blast on existing security fixtures used at nuclear installations. The second detonation would test newer protective devices and additional security barriers or vehicles.
   Source: http://www.tdn.com/articles/2005/08/18/area_news/news06.txt

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

5. *August 19, Banking Technology* — **Phishing losses at ATM machines less than feared.** Fraud losses at the ATM or point of sale (POS) resulting from phishing scams are smaller than feared according to new research from TowerGroup. The research group said there is a misconception in the marketplace that ATM or PIN−based POS debit fraud from phishing is a runaway phenomenon when, in fact, the true effect is minimal. It found that no more than $990 million was fraudulently lost at the ATM and POS in the U.S. in 2004 and of this less than one percent actually came from phishing−based fraud. After speaking to Visa, MasterCard, the FBI and five of the 10 biggest card issuing banks in the U.S., TowerGroup found that on average one in every 15,600 ATM and PIN−based POS debit transactions is fraudulent but virtually all of this fraud comes from stolen cards and card skimming. TowerGroup said it conducted its research to counter findings from Gartner at the beginning of August which estimated that ATM/POS fraud in the U.S. generated losses of $2.75 billion from phishing attacks in 2004.
   Source: http://www.bankingtech.com/ipi/bankingtech/indextemplate.jsp?pageid=article&contentid=20017308750

[Return to top]

Transportation and Border Security Sector

6. *August 21, Washington Post* — **Northwest weathers first day of strike.** Northwest Airlines Corp. encountered picket lines and some flight delays as it weathered the first day of a strike by its 4,400 mechanics and maintenance workers. The first major airline strike in seven years has set the stage for a confrontation that could reshape labor relations in a struggling industry. The airline unions, once a dominant force, have lost much of their power as their members have had to sacrifice wages and jobs repeatedly to keep the carriers afloat. With the industry in dire condition, the balance of power appears to be shifting away from organized labor to airline executives. The airline industry, facing rising fuel prices, sharp competition, an inflexible market for ticket prices and the lingering fear of terrorism, is in the midst of its most critical period in decades. Northwest was able to maintain operations largely because its other labor groups, representing pilots, flight attendants and baggage handlers, ignored the strikers and reported to work. Nevertheless, there were problems, such as a flight from Detroit to Boston scheduled to depart at 10:30 a.m. left at 4:39 p.m. because of mechanical problems. Another Detroit−to−Boston flight was delayed nearly an hour because of a problem loading luggage.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/08/20/AR2005082001238.html

7. *August 20, Associated Press* — **Thief stole 1,000 pieces of luggage from District airports.** A former Army National Guard reservist was sentenced to eight years in prison for stealing nearly 1,000 pieces of luggage at Washington, DC's three major airports. Derrick Kysar, 43, testified Friday, August 19, that he began helping himself to luggage about four years ago, eventually stealing $2 million worth of medicine, clothing, and other personal items. Kysar staked out baggage claim areas at Reagan National Airport, where he was assigned in the months after the September 11, 2001, terrorist attacks. He also targeted bags at Dulles International Airport and Baltimore Washington International Airport, selling the contents at yard sales in low−income neighborhoods. "My motive, and it's no excuse, was to pay my bills," he said, adding that he filed for bankruptcy in 1999. Investigators found hundreds of stolen items stockpiled in his Arlington home, including 300 tubes of toothpaste and 500 pairs of men's white socks. Maps, cell phones, jewelry and shoes spilled out of plastic bags and crates. Kysar stole so much stuff that he could not fit it all in his home. Inside a storage unit he rented, detectives found 60 suitcases, $870 in cash, and $680 worth of jewelry.
Source: http://www.wjla.com/news/stories/0805/253478.html

8. *August 19, Associated Press* — **Man on Amtrak train found with IDs, cash.** A man was removed from an Amtrak train for exposing himself and rummaging through other passengers' luggage. Conductors on the train from New York to Chicago alerted police, who discovered the man was carrying thousands of dollars in cash and gold and identification cards from several countries. Police took the man into custody Wednesday, August 17, at a station in Elyria, OH, about 25 miles southwest of Cleveland. The man was identified through a fingerprint check as a Canadian, Donald Thomas Sloan. In the man's bags were two Canadian passports, birth certificates, and Social Security cards with different names, a Mexican identification card, and medical records with different identities, police said.

Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/08/19/AR2005081901185.html

9. *August 19, Associated Press* — **Passengers stranded after U.S. Customs computer glitch.** A virus caused the U.S. Customs computer system used to process passengers arriving on international flights to shut down for several hours Thursday, August 18, leaving long lines of impatient travelers, officials said. Department of Homeland Security spokesperson Russ Knocke said the virus impacted computer systems at a number of airports, including those in New York, San Francisco, Miami, Los Angeles, Houston, Dallas, and Laredo, TX. The worst delays appeared to be at Miami International Airport, where as many as 2,000 people waited to clear immigration, airport spokesperson Marc Henderson said. At New York's airports, customs officials processed passengers by hand during the shutdown. In Los Angeles, they used backup computer systems to keep passengers moving. The computer problem originated in database systems located in Virginia and lasted from around 6 p.m. until about 11:30 p.m. (EDT), said Zachary Mann, spokesperson for U.S. Customs and Border Protection in southern Florida.
Source: http://www.usatoday.com/travel/news/2005−08−19−customs−computers_x.htm?POE=TRVISVA

10. *August 19, Department of Transportation* — **New rules regulating work and sleep schedules for commercial truck drivers.** The U.S. Department of Transportation's Federal Motor Carrier Safety Administration (FMCSA) on Friday, August 19, issued a new Hours−of−Service rule that spells out the length of time commercial drivers can operate trucks before they are required to take a break. The new rule replaces Hours−of−Service regulations that were last updated in 2003. Parts of the rule, including the maximum driving time and minimum rest limits remain the same. As in the 2003 regulations, the new rule prohibits truckers from driving more than eleven hours in a row, working longer than 14 hours in a shift and driving more than 60 hours over a seven day period or 70 hours over an eight day period, FMCSA Administrator Annette M. Sandberg said. In addition, the new rule requires truckers to rest for at least ten hours between shifts and provides a 34−hour period to recover from cumulative fatigue. The most important change under the new rule now allows short−haul operators not required to hold a commercial drivers license, like landscape crews and delivery drivers who work within a 150 mile radius of their starting point, to extend their work day twice a week.
Source: http://www.dot.gov/affairs/fmcsa0405.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

11. *August 21, New York Times* — **Food security threats at airports.** New York City's major international airport has stepped up watchfulness to prevent agroterrorism, or the use of biological agents against the nation's food supply. The types of food or agricultural products

that are confiscated vary from one country to another. Most of the people who run afoul of the rules are not terrorists but well−meaning travelers, who are trying to bring into the country a favorite food from home. With New York's J.F.K. airport's busiest month in full swing −− one million people typically enter there from abroad in August −− the 85 agriculture specialists who work at its five international terminals have had their hands full. "Compared to Miami, which mostly gets South American flights, and California, which mostly gets flights from Asia," Officer Mike Russo said, "what's amazing about this port is we get the world." Like a Manhattan epicure, Officer Russo ticked off some of the delicacies piled high on a steel table in the contraband room, to be ground up and incinerated after inspection: Bangladeshi jackfruit, Vietnamese pork sausage, Central American black corn, Nigerian garden eggs, Pakistani Alphonso mangoes.
Source: http://www.nytimes.com/2005/08/21/nyregion/21edib.html

12. *August 20, Casper Star Tribune (WY)* — **Horse, cattle disease cases increase.** Wyoming now has 10 cases of vesicular stomatitis (VS), spanning four counties, and the number of cases is expected to continue to rise, according to Wyoming State Veterinarian Dwayne Oldham. By Friday, August 19, four VS cases had been confirmed in Sublette County, three cases in Bighorn County, two cases in Goshen County and a single case in Washakie County. All 10 premises in the state remain under quarantine while the virus is given time to run its course. Oldham said that in addition to the 10 cases, there are "quite a few others under investigation," both within the four affected counties as well as within two other counties. VS is a sporadic, re−emerging disease characterized by blister−like lesions on the tongue, lips, oral and nasal mucosa, teats, prepuce or coronary bands of cattle, horses, and swine. Transmission of VS is not fully understood, but it is known that the disease may be spread from animal to animal or by biting insects. Clinically, VS and foot and mouth disease (FMD) look alike; therefore, laboratory tests are necessary to differentiate between them. FMD is a highly contagious foreign animal disease that can affect cloven−hoofed animals; therefore, it is very important that producers and other livestock owners report any suspect animal to their local veterinarian.
Source: http://www.casperstartribune.net/articles/2005/08/20/news/wyoming/ea22ce17dc3822458725706200827 79d.txt

13. *August 19, Stop Soybean Rust News* — **First soybean rust−like spores found in Virginia.** A single cluster of six spores matching the description of Asian soybean rust spores was collected in a spore trap in Suffolk, VA, the first sign that Phakopsora pachyrhizi spores may have traveled as far north as the Hampton Roads area in southeast Virginia. Officials retrieved the cluster from a trap at the Virginia Tech Tidewater Agricultural Research and Extension Center, where the spores had been collected in the air sampling period from August 3 to August 10. “This is a strong indication that spores of soybean rust have traveled as far north as Virginia,” said David Holshouser, soybean agronomist at the Tidewater center, “and that scouting needs to be intensified until the crop progresses through the most vulnerable stages from beginning pod up to full seed." He said weather conditions around the time of deposition (August 5−11) were “extremely hot and dry and not conducive for promoting the infection process.” Holshouser specifically said there is no indication of soybean rust in the sentinel plots adjacent to where the spores were found or in nearby soybean fields.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=514

14.

August 19, Stop Soybean Rust News — **Illinois traps soybean rust−like spores in four counties.** The twice−weekly monitoring of Illinois spore traps turned up soybean rust−like spores in four counties this week: Alexander, Warren, Massac, and St. Clair. State specialists continue to discourage Illinois growers from spraying for rust. Warren County (two spores in trap), on the Mississippi in west−central Illinois, remains the northern−most county in the U.S. reporting rust−like spores captured in a spore trap. This time around, the Alexander trap had one spore, Massac two spores and St. Clair County, five spores. Linda Kull, with the National Soybean Research Laboratory at the University of Illinois, continued to emphasize that "as of August 19, 2005, there are no observations of soybean rust on soybean, kudzu, or other potential hosts in Illinois."
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=515

15. *August 18, Fort Morgan Times (CO)* — **Rust found in sunflowers.** Rust has been identified in some commercial sunflower fields in parts of the High Plains. Rust pustules begin on the lower plant leaves and move higher during favorable conditions. Rust can be yield−impacting when the majority of the plant's leaves and bracts are covered with rust pustules. Disease development is favored by warm temperatures and wet foliage for at least 12 hours. Extended wet periods of three to four days can cause serious damage. The disease can spread very quickly under these conditions.
Source: http://www.fortmorgantimes.com/Stories/0,1413,164~8305~30162 49,00.html

[Return to top]

Food Sector

16. *August 19, USAgNet* — **Experts: Agriculture, food supply is still vulnerable to terrorism.** Terrorists aiming to spread fear, disrupt the economy and undermine confidence in the U.S. government could do all three with a focused strike on agriculture, experts said Thursday, August 18, during a conference on a surprise attack on food. The conference at the Hyatt Regency in Sacramento, CA, had particular resonance in California's Central Valley, home to six of the nation's top nine farm counties and a leading exporter of food. U.S. customs agricultural inspector Tracy Encinas has seen the range of potential threats expand along the border in Nogales, AZ, where 70 percent of winter produce enters the United States. "At the port level, there's been more of a focus on weapons of mass destruction and persons of interest," she said. "But now there's more of a focus on agriculture." Speakers, including John Hoffman, the U.S. Department of Homeland Security's top food and agricultural officer, said "food defense" has increasingly become a higher priority for funding, law enforcement bureaucracy and government planning.
2005 Agroterrorism Assembly: http://www.aon.com/us/about/events/agroterrorism.jsp
Source: http://www.usagnet.com/story−national.cfm?Id=835&yr=2005

[Return to top]

Water Sector

17.

August 20, New York Times — **Tainted water at state park claims victims in 20 counties.** New York state health officials said Friday, August 19, that the number of people who contracted a severe intestinal illness from a play area with sprinklers at Seneca Lake State Park in Geneva, has soared to 1738. The outbreak of the disease, a parasitic waterborne infection called cryptosporidiosis, began about two months ago among visitors to the state park but went unnoticed until earlier this week, health officials said. Almost all those who were infected had spent time at a popular water attraction, the Sprayground, and were exposed to tainted water. On Monday, August 15, the Sprayground, a popular spot for families and day camps that gets about 40,000 visitors every August, was closed for the rest of the summer by park officials. They decided to close after health officials, acting on reports of a surge in cases of cryptosporidiosis from four counties, determined that the water might be contaminated. After an investigation, they found two separate tanks that feed the play area with water from a nearby town contained water tainted with protozoa that cause cryptosporidiosis. But they have not figured out how the parasites survived in the tanks, both equipped with chlorination and filtration systems.
Source: http://www.nytimes.com/2005/08/20/nyregion/20sick.html

18. *August 19, Associated Press* — **San Francisco boosts water system's security.** San Francisco, California's mayor announced a partnership Thursday, August 18, between the city and the National Parks Service to enhance security and environmental protection of the watershed that provides the Bay Area most of its water. About 2.4 million customers in the San Francisco Bay area get their water through the 167−mile aqueduct, which extends from Yosemite National Park to San Francisco. Mayor Gavin Newsom discussed a five−year, $15 million plan for the watershed that includes maintenance of trails and camping areas, as well as security improvements within the park. Newsom also announced the establishment of a new position within the city's Public Utilities Commission. Greg Suhr, currently with the San Francisco Police Department, will be the commission's new chief of security starting September 6. He will spend his first two months in office reviewing the commission's plan for dealing with emergencies along the regional water system.
Source: http://www.thedesertsun.com/apps/pbcs.dll/article?AID=/20050819/NEWS10/508190331/1024

[Return to top]

Public Health Sector

19. *August 20, Washington Post* — **Soviet germ factories pose new threat.** There are more than 80 "antiplague" labs scattered across the former Soviet Union. Each is a repository of knowledge, equipment, and lethal pathogens that weapons experts have said could be useful to bioterrorists. "They often have culture collections of pathogens that lack biosecurity, and they employ people who are well−versed in investigating and handling deadly pathogens," said Raymond Zilinskas, a bioweapons expert and coauthor of the draft report on the antiplague system. "Some are located at sites accessible to terrorist groups and criminal groups. The potential is that terrorists and criminals would have little problem acquiring the resources that reside in these facilities." Since the collapse of the Soviet Union in 1991, budgets at the institutes have fallen so steeply that even the simplest security upgrades are out of reach. One facility in a Central Asian capital could not even afford a telephone and had no way of

contacting police in the event of a break−in. At least two antiplague centers outside Russia have acknowledged burglaries or break−ins within the past three years, though there are no confirmed reports of stolen pathogens or missing lab equipment. The lack of modern biosafety equipment is also raising concern among U.S. officials about the potential for an accidental release of deadly bacteria and viruses.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/08/19/AR2005081901507.html

20. *August 19, Agence France−Presse* — **Flu vaccine production capacity inadequate in emergency.** The World Health Organization (WHO) has warned that the global capacity to manufacture anti−flu vaccines would not be flexible or large enough to counter a threatened pandemic that could rapidly kill millions of people around the world. "Current global manufacturing capacity... is inadequate to meet the expected global needs during a pandemic and cannot be rapidly augmented," the WHO said Friday, August 19, in a weekly bulletin on disease outbreaks and threats. The H5N1 virus has killed more than 60 people who were infected by chickens and birds in Asia since 2003. The strain is regarded as the most likely current source of a more virulent form of the human flu virus that could mutate and spread rapidly around the world, potentially killing millions of people. Any major production shift towards the H5N1 vaccine would also compromise protection against regular, seasonal influenza, the WHO added. Seasonal epidemics of flu cause an estimated 250,000 to 500,000 deaths a year, according to the WHO. Ninety percent of production capacity for all influenza vaccines −− 300 million doses −− is concentrated in Europe and North America. Production there was likely to meet domestic demand for flu vaccines or treatments first even in an emergency.
WHO Weekly epidemiological record: http://www.who.int/wer/2005/wer8033.pdf
Source: http://news.yahoo.com/s/afp/20050819/hl_afp/healthfluwhovaccinepandemic_050819163646;_ylt=AuPeW3qbAh8sKf4.xh4FRc2JOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

21. *August 19, Dakota Voice (SD)* — **South Dakota West Nile virus cases near 50.** The South Dakota Department of Health on Friday, August 19, reported 13 new human West Nile virus (WNV) detections, including 12 new cases and one new blood donor detection. This brings to 48 the number of human WNV detections this season. New detections were reported in Brown, Campbell, Codington, Davison, Grant, Hamlin, Hanson, Moody, Spink, and Stanley counties. In addition, 20 positive Culex mosquito pools were detected in Beadle, Brookings, and Hughes counties. Thirty−three of South Dakota's 66 counties have now had WNV detections. Provisional data shows that the median age of the South Dakota cases is 43 years, with the range from 14 to 80 years old. Ninety−five percent of cases are white and five percent are American Indian. Of the cases fully investigated, 16 percent have had WNV neuroinvasive disease and 84 percent have had WNV fever. At this time last year South Dakota had reported 18 cases. Nationally, 42 of the 48 continental states have had WNV detections, with 24 states reporting a total of 333 human WNV cases, 76 blood donors, and three deaths. At this time in 2004, 689 human cases had been reported nationally.
Source: http://www.dakotavoice.com/200508/20050819_3.asp

22. *August 19, Associated Press* — **Arkansas pet distributor quarantined.** The Arkansas Department of Health and Human Services ordered a pet store distributing company

quarantined Friday, August 19, after officials suspected some of the store's rodents were infected with a virus that can be harmful to humans. Midsouth Distributors of Arkansas LLC near Scott was also prohibited from selling and distributing animals to pet stores and consumers and ordered to allow testing of some of its animals for the lymphocytic choriomeningitis virus (LCMV). In Massachusetts and Rhode Island, three people died after receiving organ transplants from a donor who tested positive for LCMV. The organ donor owned a hamster that was bought from Midsouth Distributors of Ohio LLC, which has common ownership with Midsouth Distributors of Arkansas LLC, the Arkansas officials said. The Ohio facility allowed the U.S. Centers for Disease Control and Prevention test their hamsters and guinea pigs for the virus after the deaths. The tests results showed that two hamsters, which had arrived from the Arkansas facility, were infected with LCMV. A third was found to have had the infection in the past.
LCMV information: http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/lcmv.htm
Source: http://www.boston.com/news/local/rhode_island/articles/2005/08/19/arkansas_pet_distributor_quarantined/

23. *August 16, University of Washington* — **Study reveals a way disease bacteria sense antimicrobials and initiate a counter−defense.** Many living things, from fruit flies to people, naturally produce disease−fighting chemicals, called antimicrobial peptides, to kill harmful bacteria. In a counter move, some disease−causing bacteria have evolved microbial detectors. The bacteria sense the presence of antimicrobial peptides as a warning signal. The alarm sets off a reaction inside the bacteria to avoid destruction. University of Washington (UW) and McGill University researchers have revealed a molecular mechanism whereby bacteria can recognize tiny antimicrobial peptide molecules, then respond by becoming more virulent. Their studies were done on the bacterium Salmonella typhimurium. Strangely enough, the same molecules that the body sends out to help destroy salmonella inadvertently launch bacterial defenses. It is as if missiles armed, rather than demolished, the target. The body's antimicrobial peptides bind to an enzyme, PhoQ, which acts as a watchtower and interceptor near the surface of bacterial cell membranes. The peptide binding activates PhoQ, which sets off a cascade of signals. The signals turn on a large set of bacterial genes. Some of the genes are responsible for products that fortify the bacterial cell surface and protect the bacteria from being killed.
Source: http://www.uwnews.org/article.asp?articleID=11694

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

24. *August 19, The McDowell News (NC)* — **Simulated terror attack will be North Carolina's biggest drill.** Hundreds of emergency workers from 15 counties in North Carolina participated in a mock terrorist attack that took place in McDowell County, NC, Sunday, August 21. Through a grant provided by the Department of Homeland Security (DHS) and the North

Carolina Division of Emergency Management, EnviroSafe Consulting and Investigations Inc. of Graham, NC, managed the project that simulated a regional response to a large−scale terrorism event. The exercise kicked off at 1 p.m. at McDowell High School and ran until 5 p.m. that evening. McDowell County Emergency Services Director Carroll Hemphill said the scenario involved mass casualties caused by a chemical product emitted into the air. There was participation from approximately 50 "victims" and 350 emergency and law enforcement personnel from local, state and federal agencies in McDowell, Buncombe, Burke, Watauga, Mitchell, Avery, Yancey, Henderson, Haywood, Madison, Swain, Jackson, Rutherford and other nearby North Carolina counties. "This is the largest training exercise McDowell County has ever done and it will be the largest exercise in the state for 2005," according to Hemphill.
Source: http://www.mcdowellnews.com/servlet/Satellite?pagename=MMN/MGArticle/MMN_BasicArticle&c=MGArticle&cid=1031784540119

25. *August 18, 13 WVEC (VA)* — **Drill simulates response to nuclear attack in South Carolina.** Troops at Fort Monroe in Hampton, VA, are conducting exercises this week to simulate response to a 10−kiloton nuclear device that explodes in Veteran's Pier in Charleston, SC. In the mock attack, 10,000 people have died and nearly 100,000 have been injured. It's the job of the Joint Task Force Civil Support to coordinate aid and resources for the area. If a nuclear attack were to happen, this practice is critical so all federal, state and local agencies clearly understand their role in the relief effort. "We are specifically designed as a part of U.S. Northern Command to come in after an incident like this and assist local responders with saving lives, preventing further injuries and restoring critical life support," noted Major General Bruce Davis. That support means everything from organizing supplies to flying in extra medical staff and clean−up crews. These exercises are taking place at sites around the country to help agencies prepare for 15 different scenarios.
Source: http://www.wvec.com/news/military/stories/wvec_military_081805_terror_drill_monroe.87bc02cc.html

26. *August 18, The Suburban (NJ)* — **First responders to share soldiers' high−tech tools in New Jersey.** Fort Monmouth, NJ's, civilian engineers are now custom designing some technical communication devices relied on by soldiers in battle for use by first responders. Fort Monmouth Fire Chief John C. Erichsen and members of his department, along with Fort Monmouth police and rescue units, recently joined engineers from the U.S. Army's Communications−Electronics, Research, Development and Engineering Center (CERDEC) in demonstrating some of those technologies outside of the laboratories on base where they first were created. The various devices, known collectively as The First Responder−Response Operations Center (ROC), were developed by CERDEC's Space and Terrestrial Communications Directorate (S&TCD). Using the ROC to maintain contact between rescuers and command posts as well as among various police, fire, and rescue units at a scene should be "standard operating procedure within five years," according to Erichsen. One option first responders could become accustomed to is the "HazBot" −− a robot operated remotely from the ROC can be used to detect chemicals or poisons through sensors and cameras prior to rescuers entering a disaster area. Any samples of hazardous materials can then be transmitted using the ROC's satellite equipment to the Center for Disease Control (CDC) for identification.
Source: http://suburban.gmnews.com/news/2005/0818/Front_Page/042.htm l

27.

August 18, Information Week — **Military selects new technology to improve terrorism readiness.** Four years after the September 11 terrorist attacks, one of the toughest issues still facing emergency−response teams is how they can communicate and react most effectively amid the chaos of a disaster scene. The U.S. military expects three key technologies it tested earlier this summer can be put to use to help coordinate homeland defense efforts among military, government, and civilian agencies. The U.S. Northern Command (Northcom) is pushing for additional funding and deployment of three communications and information technologies that it evaluated in June. Northcom has high hopes for the selected systems to help emergency−response teams collaborate during a weapons−of−mass−destruction attack, communicate in real−time across classified and unclassified networks, and let responders speak to each other over previously incompatible radios. The technology selected were the Weapons of Mass Destruction Common Operational Picture (WMD COP), the Multi−level−secure Information Infrastructure (MI2), and the Incident Commander's Radio Interface (ICRI). Now that Northcom, which the Defense of Department (DoD) created in 2002, has confirmed its interest in these technologies, the next hurdle is getting them into the field where they can help troops and emergency responders.
Source: http://informationweek.com/story/showArticle.jhtml?articleID =169400172

28. *August 18, Quad−City Times (IL)* — **Mock disaster drill tests airport response in Illinois.** At a mock disaster drill hosted by the Quad−City International Airport in Illinois −− a drill the Federal Aviation Administration (FAA) requires to be conducted every three years −− about 60 people were "killed" or "injured" in an airplane crash and two dump trucks were said to be on fire. "The purpose of this exercise is to make certain that everyone working at the airport and in each of our responding mutual aid organizations knows the disaster plan, and knows exactly what to do," said Mike Swanson, the airport's public safety manager. Moline, IL, firefighter Scott Houzenga explained rescuers used the triage system in the emergency. After the crash, paramedics went around and quickly evaluated injuries to decide which people could be saved, and which could not. About 24 emergency groups participated in the mock drill. "This exercise is important for all organizations because it can help save lives in a real emergency," said Bruce Carter, director of aviation at the airport. The Quad−City International Airport serves more than 800,000 passengers annually with five carriers and is the third largest airport in Illinois.
Source: http://www.qctimes.net/articles/2005/08/18/news/local/doc4304d10d39c6f954929432.txt

[Return to top]

Information Technology and Telecommunications Sector

29. *August 19, IDG News Service* — **German government launches national IT security plan.** The German government aims to counter the alarming rise in computer viruses with a national IT security plan that includes the establishment of a computer emergency response center. The new plan was unveiled Thursday, August 18, in Berlin by Interior Minister Otto Schily. The German government's "National Plan to Protect IT Infrastructures" has three major focuses: early prevention, swift response and security standards. The Federal Office for Security in Information Technology (BSI) will play a key role. It will be responsible for developing and implementing new security standards in the public sector, and publishing guidelines for the private sector. BSI will also house the computer emergency response center, which will

collaborate with providers of IT security services in the private sector. Among the planned tasks of the center: sending e−mail alerts about potential threats and responding to attacks with hotline technical support.
The German IT security plan is available in German on the ministry's Website at:
http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/Nationaler__Plan__Schutz__Informationsinfrastrukturen,templateId=raw,property=publicationFile.pdf/Nationaler_Plan_Schutz_Informa tionsinfrastrukturen.
Source: http://www.infoworld.com/article/05/08/19/HNgermansecurity_1.html?source=rss&url=http://www.infoworld.com/article/05/08/ 19/HNgermansecurity_1.html

30. *August 18, FrSIRT* — **MailWatch for MailScanner XML−RPC remote code execution issue.** A vulnerability was identified in MailWatch for MailScanner, which could be exploited by remote attackers to execute arbitrary code. This flaw is due to an input validation error in the XML−RPC library when processing, via an "eval()" call, certain XML tags nested in parsed documents, which could be exploited by remote attackers to execute arbitrary PHP commands. For additional information, see : FrSIRT/ADV−2005−1413 Products affected are MailWatch for MailScanner versions prior to 1.0.2.
Users should upgrade to MailWatch for MailScanner version 1.0.2:
http://mailwatch.sourceforge.net/
Source: http://www.frsirt.com/english/advisories/2005/1457

31. *August 18, zone−h* — **Juniper Netscreen VPN: username enumeration vulnerability.** NTA Monitor has discovered a VPN username enumeration vulnerability in the Juniper Netscreen integrated Firewall/VPN products while performing a VPN security test for a customer. The vulnerability affects remote access VPNs (known as "Dialup VPNs" in ScreenOS) using IKE with pre−shared key authentication. Certificate authentication is not affected, nor is manual key authentication. In practice, we find that most Netscreen systems are configured for remote access with pre−shared key authentication (called "AutoKey IKE with Preshared keys" in ScreenOS), so this bug will affect the majority of users. The vulnerability allows an attacker to use a dictionary attack to determine valid VPN usernames on the Netscreen. Once a valid username is discovered, the attacker can then use this to obtain a hash from the Netscreen, which can then be cracked offline to determine the associated password. Once an attacker has a valid username and password, they can potentially gain access to the resources protected by the VPN. The issue is believed to affect all models of Juniper Netscreen running all ScreenOS software versions up to 5.2.0. Users should use certificate authentication rather than pre−shared key authentication.
Source: http://www.zone−h.org/advisories/read/id=7977

32. *August 18, FrSIRT* — **PHPTB "absolutepath" remote PHP file inclusion vulnerability.** A vulnerability was identified in PHPTB, which may be exploited by attackers to compromise a vulnerable web server. This flaw is due to an input validation error in the "admin_o.php" script when processing a specially crafted "absolutepath" parameter, which may be exploited by remote attackers to include malicious files and execute arbitrary commands with the privileges of the Web server. Products affected are PHPTB version 2.0 and prior. The FrSIRT is not aware of any official supplied patch for this issue.
Source: http://www.frsirt.com/english/advisories/2005/1460

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a public exploit for a vulnerability in the Microsoft DDS Library Shape Control (msdds.dll) component, which comes with various Microsoft products such as Visual Studio .NET and Microsoft Office. Systems with Visual Studio .NET 2002, which installs msdds.dll version 7.0.9466.0, are vulnerable. Based on initial testing, msdds.dll version 7.10.3077.0 does not appear vulnerable. This version of the dll is installed with Office 2003 and Visual Studio .NET 2003. Although MS Office XP provides a vulnerable version of msdds.dll, it does not appear that IE will instantiate the COM object in question with the standard installation.

By convincing a user to view an HTML document (e.g., a web page or an HTML email message) that attempts to instantiate the Microsoft DDS Library Shape Control COM object, a remote attacker could execute arbitrary code on the user's system with privileges of the user. More information about this vulnerability can be found in the following US−CERT Vulnerability Note:

VU#740372 − Microsoft DDS Library Shape Control (msdds.dll) COM object contains an unspecified vulnerability

This vulnerability has similar characteristics to the previously posted javaprxy.dll vulnerability (VU#939605). The underlying vulnerability is that Internet Explorer will instantiate non−ActiveX COM objects that are referenced in an HTML document. This can cause Internet Explorer to crash. More information about this vulnerability can be found in the following US−CERT Vulnerability Note:

VU#680526 − Microsoft Internet Explorer allows non−ActiveX COM objects to be instantiated

Until a patch is available to address this vulnerability, US−CERT strongly encourages users to review the workarounds section of Vulnerability Note (VU#740372). Additionally, Microsoft has published a Security Advisory about this issue and is continuing to investigate the problem.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 1026 (−−−), 6881 (bittorrent), 135 (epmap), 139 (netbios−ssn), 1433 (ms−sql−s), 4004 (pxc−roid), 6346 (gnutella−svc), 25 (smtp), 80 (www) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

33. *August 19, Grand Forks Herald (ND)* — **Drill uncovers weak spots in school's security.** Installing more security cameras and buying two−way radios to be used during emergencies were two of the ideas that came out of a school−violence drill Thursday, August 18, at Red River High School in Grand Forks, ND. Dozens of first responder personnel, from police officers to the bomb squad, and ambulance workers, converged on the school as part of an exercise to test school and community policies and procedures for responding to an intentional act of violence at one of the schools or other school facilities. In the exercise, two armed intruders entered the school, which went into a lockdown once the intruders were discovered. Law enforcement and other agencies were summoned, and officers came in and "apprehended the bad guys," said Jody Thompson, assistant superintendent for elementary education for the Grand Forks Public Schools. The exercise was followed by a debriefing at which law enforcement, medical personnel, school officials and others discussed how the exercise went and what it revealed about security at the schools. "I think there's always the opportunity for improving communications, especially when you're talking about agencies that in the past haven't worked together," Thompson said.
Source: http://www.grandforks.com/mld/grandforks/news/12421051.htm

34. *August 19, Associated Press* — **Threat prompts security alert at Rome's Coliseum.** Tourists visiting Rome's ancient Coliseum will first make their way through metal detectors, X−ray machines, closed−circuit cameras, and barriers because of a heightened threat of terrorism, officials said Friday, August 19. Most of the measures were added to the Coliseum about two weeks ago, said Liliana Ferraro, who oversees security for Rome's city council. The metal barriers are expected to go up next week around the monument's entrances and will help keep lines orderly and the illegal vendors away, Ferraro said. The extra security was not a response to a specific threat at the monument, which is Italy's most popular tourist destination and receives about 16,000 visitors a day, she said. Pilgrims and tourists already pass through metal detectors at St. Peter's Basilica and Rome's Capitoline Museums.
Source: http://www.usatoday.com/news/world/2005−08−19−rome−security_x.htm

[Return to top]

General Sector

35. *August 20, Associated Press* — **Concern grows over prison Islam converts.** Recent arrests have focused attention on a potential terrorism danger that federal officials have been warning about −− that inmates in state prison systems are particularly susceptible to radical Islamist ideology. But prison officials across the nation say they so far have seen more potential for recruitment than real threats. Federal officials have arrested three men in Southern California

since early July in a plot that allegedly targeted National Guard facilities, the Israeli Consulate in Los Angeles and several synagogues. Authorities said they believe the plan originated among a shadowy group known as Jamiyyat Ul Islam Is Saheeh inside California State Prison, Sacramento. Counterterrorism officials said the danger is not in the number of adherents to radical Islam but in the potential for small groups of dedicated believers to commit terrorist acts after they are released. They point to Jose Padilla, an American Muslim convert arrested in 2002 for allegedly planning a "dirty bomb" radiological attack after he left jail. In a report last year, the U.S. Department of Justice's inspector general found that the federal Bureau of Prisons was doing inadequate background or ideology checks on its Muslim clerics. It found that inmates and religious volunteers had "ample opportunity ... to deliver inappropriate and extremist messages without supervision."
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/08/20/AR2005082000689.html

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer